# ECHELON
# The NSA's Global Spying Network

***The US National Security Agency uses the ECHELON system not only for surveillance of civilians and politicians, but also for spying on behalf of US corporations.***

***Part 2 of 2***

**by Patrick S. Poole © 1998/99**

E-mail: pspoole@hiwaay.net
Website: http://fly.hiwaay.net/~pspoole/echelon.html

A fundamental foundation of free societies is that when controversies arise over the assumption of power by the state, power never defaults to the government, nor are powers granted without an extraordinary, explicit and compelling public interest. As the late United States Supreme Court Justice William Brennan pointed out:

> *The concept of military necessity is seductively broad and has a dangerous plasticity. Because they invariably have the visage of overriding importance, there is always a temptation to invoke security "necessities" to justify an encroachment upon civil lib - erties. For that reason, the military-security argument must be approached with a healthy skepticism: its very gravity counsels that courts be cautious when military necessity is invoked by the Government to justify a trespass on [Constitutional] rights.*[32]

Despite the necessity of confronting terrorism and the many benefits that are provided by the massive surveillance efforts embodied by ECHELON, there is a dark and dangerous side of these activities that is concealed by the cloak of secrecy surrounding the intelligence operations of the United States.

The discovery of domestic surveillance targeting American civilians for reasons of "unpopular" political affiliation or for no probable cause at all—in violation of the First, Fourth and Fifth Amendments of the Constitution—is regularly impeded by very elaborate and complex legal arguments and privilege claims by the intelligence agencies and the US Government. The guardians and caretakers of our liberties—our duly elected political representatives—give scarce attention to the activities, let alone the abuses, that occur under their watch. As pointed out below, our elected officials frequently become targets of ECHELON themselves, chilling any effort to check this unbridled power.

In addition, the shift in priorities resulting from the demise of the Soviet Empire, and the necessity to justify intelligence capabilities, resulted in a redefinition of "national security interests" to include espionage committed on behalf of powerful American companies. This quiet collusion between political and private interests typically involves the very same companies that are involved in developing the technology that empowers ECHELON and the intelligence agencies.

## DOMESTIC AND POLITICAL SPYING

When considering the use of ECHELON on American soil, the pathetic historical record of NSA and CIA domestic activities in regard to the Constitutional liberties and privacy rights of American citizens provides an excellent guidepost for what may occur now with the ECHELON system. Since the creation of the NSA by President Truman, its spying capability has frequently been used to monitor the activities of an unsuspecting public.

### Project SHAMROCK

In 1945, Project SHAMROCK was initiated to obtain copies of all telegraphic information exiting or entering the United States. With the full cooperation of RCA, ITT and Western Union (representing almost all of the telegraphic traffic in the US at the time), the NSA's predecessor and later the NSA itself were provided with daily microfilm copies of all incoming, outgoing and transiting telegraphs. This system changed dramatically when the cable companies began providing magnetic computer tapes to the agency, which enabled the agency to run all the messages through its HARVEST computer to look for

particular keywords, locations, senders or addressees.

Project SHAMROCK became so successful that in 1966 the NSA and CIA set up a front company in lower Manhattan (where the offices of the telegraph companies were located) under the code-name LPMEDLEY. At the height of Project SHAMROCK, 150,000 messages a month were printed and analysed by NSA agents.[33]

NSA Director Lew Allen brought Project SHAMROCK to a crashing halt in May 1975 as congressional critics began to rip open the program's shroud of secrecy. The testimony of both the representatives from the cable companies and Director Allen at the hearings prompted Senate Intelligence Committee chairman Senator Frank Church to conclude that Project SHAMROCK was "probably the largest government interception program affecting Americans ever undertaken".[34]

### Project MINARET

A sister project to Project SHAMROCK, Project MINARET involved the creation of "watch lists", by each of the intelligence agencies and the FBI, of those accused of "subversive" domestic activities. The watch lists included such notables as Martin Luther King, Malcolm X, Jane Fonda, Joan Baez and Dr Benjamin Spock.

After the Supreme Court handed down its 1972 Keith decision[35]— which held that, while the President could act to protect the country from unlawful and subversive activity designed to overthrow the government, that same power did not extend to include warrantless electronic surveillance of domestic organisations—pressure came to bear on Project MINARET.[36] Attorney-General Elliot Petersen shut down Project MINARET as soon as its activities were revealed to the Justice Department, despite the fact that the FBI (an agency under the Justice Department's authority) was actively involved with the NSA and other intelligence agencies in creating the watch lists.

**This quiet collusion between political and private interests typically involves the very same companies that are involved in developing the technology that empowers ECHELON and the intelligence agencies.**

Operating between 1967 and 1973, over 5,925 foreigners and 1,690 organisations and US citizens were included on the Project MINARET watch lists. Despite extensive efforts to conceal the NSA's involvement in Project MINARET, NSA Director Lew Allen testified before the Senate Intelligence Committee in 1975 that the NSA had issued over 3,900 reports on the watch-listed Americans.[37] Additionally, the NSA Office of Security Services maintained reports on at least 75,000 Americans between 1952 and 1974. This list included the names of anyone who was mentioned in an NSA message intercept.

### Operation CHAOS

While the NSA was busy snooping on US citizens through Projects SHAMROCK and MINARET, the CIA got into the domestic spying act by initiating Operation CHAOS. President Lyndon Johnson authorised the creation of the CIA's Domestic Operations Division (DOD), whose purpose was to "exercise centralised responsibility for direction, support and coordination of clandestine operations activities within the United States".

When Johnson ordered CIA Director John McCone to use the DOD to analyse the growing college student protests against the Administration's policy towards Vietnam, two new units were set up to target anti-war protesters and organisations: Project RESISTANCE, which worked with college administrators, campus security and local police to identify anti-war activists and political dissidents; and Project MERRIMAC, which monitored any demonstrations being conducted in the Washington, DC, area. The CIA then began monitoring student activists and infiltrating anti-war organisations by working with local police departments to pull-off burglaries, illegal entries (black bag jobs), interrogations and electronic surveillance.[38] After President Nixon came to office in 1969, all of these domestic surveillance activities were consolidated into Operation CHAOS.

After the revelation of two former CIA agents' involvement in the Watergate break-in, the publication of an article about CHAOS in the *New York Times*[39] and the growing concern about distancing itself from illegal domestic spying activities, the CIA shut down Operation CHAOS. But during the life of the project, the Church Committee and the Commission on CIA Activities Within the United States (the Rockefeller Commission) revealed that the CIA had compiled files on over 13,000 individuals, including 7,000 US citizens and 1,000 domestic organisations.[40]

### The Foreign Intelligence Surveillance Court (FISC)

In response to the discovery of such a comprehensive effort by previous administrations and the intelligence agencies, Congress passed legislation (the Foreign Intelligence Surveillance Act of 1978)[41] that created a top-secret court, the Foreign Intelligence Surveillance Court (FISC), to hear applications for electronic surveillance from the FBI and NSA to provide some check on the domestic activities of the agencies. In 1995, Congress granted the court additional power to authorise surreptitious entries. In all of these actions, congressional intent was to provide a check on the domestic surveillance abuses mentioned above.

The seven-member court, comprised of Federal District Court judges appointed by the Supreme Court Chief Justice, sits in secret in a sealed room on the top floor of the Department of Justice building. Public information about the FISC's hearings is scarce, but each year the Attorney-General is required by law to transmit to Congress a report detailing the number of applications each year and the number granted.

With over 10,000 applications submitted to the FISC during the past 20 years, the court has only rejected one application (and that rejection was at the request of the Reagan Administration, which had submitted the application).

While the FISC was established to be the watchdog for the Constitutional rights of the American people against domestic surveillance, it quickly became the lap dog of the intelligence agencies. Surveillance requests that would never receive a hearing in a state or federal court are routinely approved by the FISC. This has allowed the FBI to use the process to conduct surveillance to obtain evidence in circumvention of the US Constitution, the evidence then being used in subsequent criminal trials. But the process established by Congress and the courts ensures that information regarding the cause or extent of the surveillance order is withheld from defence attorneys because of the classified nature of the court.[42] Despite Congress's initial intent for the FISC, it is doubtful that domestic surveillance by means of ECHELON comes under any scrutiny by the court.

## POLITICAL USES OF ECHELON AND UKUSA

Several incidents of domestic spying involving ECHELON have emerged from the secrecy of the UKUSA relationship. What these brief glimpses inside the intelligence world reveal is that, despite the best of intentions by elected representatives, presidents and prime ministers, the temptation to use ECHELON as a tool of political advancement and repression proves too strong.

Former Canadian spy Mike Frost recounts how former British Prime Minister Margaret Thatcher made a request in February 1983 to have two ministers from her own government monitored when she suspected them of disloyalty. In an effort to avoid the legal difficulties involved with domestic spying on high-level governmental officials, the GCHQ liaison in Ottawa made a request to CSE for them to conduct the three-week-long surveillance mission at British taxpayer expense. Frost's CSE boss, Frank Bowman, travelled to London to do the job himself. After the mission was over, Bowman was instructed to hand over the tapes to a GCHQ official at head office.[43]

Using the UKUSA alliance as legal cover is seductively easy. As *Spyworld* co-author Michel Gratton puts it:

"The Thatcher episode certainly shows that GCHQ, like NSA, found ways to put itself above the law and did not hesitate to get directly involved in helping a specific politician for her personal political benefit…

"[T]he decision to proceed with the London caper was probably not put forward for approval to many people up the bureaucratic ladder. It was something CSE figured they would get away with easily, so checking with the higher-ups would only complicate things unnecessarily."[44]

**Seemingly non-controversial organisations have ended up in the fixed gaze of ECHELON... Among the targeted organisations...were Amnesty International, Greenpeace, and Christian Aid...**

Frost also told of how he was asked in 1975 to spy on an unlikely target: Prime Minister Pierre Trudeau's wife, Margaret Trudeau. The Royal Canadian Mounted Police's (RCMP) Security Service division was concerned that the Prime Minister's wife was buying and using marijuana, so they contacted the CSE to do the dirty work. Months of surveillance in cooperation with the Security Service turned up nothing of note. Frost was concerned that there were political motivations behind the RCMP's request: "She was in no way suspected of espionage. Why was the RCMP so adamant about this? Were they trying to get at Pierre Trudeau for some reason or just protect him? Or were they working under orders from their political masters?"[45]

The NSA frequently gets into the political spying act as well. Nixon presidential aide John Ehrlichman revealed in his published memoirs, *Witness to Power: The Nixon Years*, that Henry Kissinger used the NSA to intercept the messages of then-Secretary of State William P. Rogers, which Kissinger used to convince President Nixon of Rogers' incompetence. Kissinger also found himself on the receiving end of the NSA's global net. Word of Kissinger's secret diplomatic dealings with foreign governments would reach the ears of other Nixon administration officials, incensing Kissinger. As former NSA Deputy Director William Colby pointed out: "Kissinger would get sore as hell...because he wanted to keep it politically secret until it was ready to launch."[46]

However, elected representatives have also become targets of spying by the intelligence agencies. In 1988, Margaret Newsham, a former Lockheed software manager who was responsible for a dozen VAX computers that powered the ECHELON computers at Menwith Hill, came forth with the stunning revelation that she had actually heard the NSA's real-time interception of phone conversations involving South Carolina Senator Strom Thurmond. Newsham was fired from Lockheed after she filed a whistleblower lawsuit alleging that the company was engaged in flagrant waste and abuse. After a top-secret meeting in April 1988 with then Chairman of the House Permanent Select Committee on Intelligence, Rep. Louis Stokes, Capitol Hill staffers familiar with the meeting leaked the story to the Cleveland *Plain Dealer*.[47] While Sen. Thurmond was reluctant to pressure for a thorough investigation into the matter, his office revealed at the time that it had previously received reports that the Senator was a target of the NSA.[48] After the news reports, an investigation into the matter discovered that there were no controls or questioning over who could enter target names into the Menwith Hill system.[49]

The NSA, under orders from the Reagan Administration, also targeted Maryland Congressman Michael Barnes. Phone calls he placed to Nicaraguan officials were intercepted and recorded, including a conversation he had with the Foreign Minister of Nicaragua, protesting the implementation of martial law in that country. Barnes found out about the NSA's spying after White House officials leaked transcripts of his conversations to reporters. CIA Director William Casey, later implicated in the Iran-Contra affair, showed Barnes a Nicaraguan Embassy cable that reported a meeting between embassy staff and one of Barnes' aides. The aide had been there on a professional call regarding an international affairs issue, and Casey asked for Barnes to fire the aide. Barnes replied that it was perfectly legal and legitimate for his staff to meet with foreign diplomats.

Barnes commented: "I was aware that NSA monitored international calls, that it was a standard part of intelligence gathering. But to use it for domestic political purposes is absolutely outrageous and probably illegal."[50]

Another former chairman of the Senate Intelligence Committee has also expressed his concerns about the NSA's domestic targeting. "It has always worried me. What if that is used on American citizens?" queried former Arizona Senator Dennis DeConcini. "It is chilling. Are they listening to my private conversations on my telephone?"[51]

Seemingly non-controversial organisations have ended up in the fixed gaze of ECHELON, as several former GCHQ officials confidentially told the London *Observer* in June 1992. Among the targeted organisations they named were Amnesty International, Greenpeace, and Christian Aid—an American missionary organisation that works with indigenous pastors engaged in ministry work in countries closed to Western, Christian workers.[52]

In another story published by the London *Observer*, a former employee of the British Joint Intelligence Committee, Robin Robison, admitted that Margaret Thatcher had personally ordered the communications interception of Lonrho, the parent company of the *Observer*, after the *Observer* had published a 1989 exposé charging that bribes had been paid to Thatcher's son, Mark, in a multibillion-dollar British arms deal with Saudi Arabia. Despite facing severe penalties for violating his indoctrination vows, Robison admitted that he had personally delivered intercepted Lonrho messages to Mrs Thatcher's office.[53]

It should hardly be surprising that ECHELON ends up being used by elected and bureaucratic officials to their political advantage or by the intelligence agencies themselves for the purpose of sustaining their privileged surveillance powers and bloated budgets. The availability of such invasive technology practically begs for abuse, although it does not justify its use to those ends. But what is most frightening is the targeting of such "subversives" as those who expose corrupt government activity, protect human rights from government encroachments, challenge corporate polluters or promote the Gospel of Christ. That the vast intelligence powers of the United States should be arrayed against legitimate and peaceful organisations is demonstrative not of the desire to monitor, but of the desire to control.

## COMMERCIAL SPYING

With the rapid erosion of the Soviet Empire in the early 1990s, Western intelligence agencies were anxious to redefine their mission to justify the scope of their global surveillance system. Some of the agencies' closest corporate friends quickly gave them an option: commercial espionage. By redefining the term "national security" to include spying on foreign competitors of prominent US corporations, the signals intelligence game has got uglier. And this may very well have prompted the recent scrutiny by the European Union that ECHELON has endured.

While UKUSA agencies have pursued economic and commercial information on behalf of their countries with renewed vigour after the passing of communism in Eastern Europe, the NSA practice of spying on behalf of US companies has a long history.

**While UKUSA agencies have pursued economic and commercial information on behalf of their countries with renewed vigour after the passing of communism, the NSA practice of spying on behalf of US companies has a long history.**

Gerald Burke, who served as Executive Director of President Nixon's Foreign Intelligence Advisory Board, notes commercial espionage was endorsed by the US Government as early as 1970: "By and large, we recommended that, henceforth, economic intelligence be considered a function of the national security, enjoying a priority equivalent to diplomatic, military and technological intelligence."[54]

To accommodate the need for information regarding international commercial deals, the intelligence agencies set up a small, unpublicised department within the Department of Commerce: the Office of Intelligence Liaison. This office receives intelligence reports from the US intelligence agencies about pending international deals that it discreetly forwards to companies that request it or may have an interest in the information.

Immediately after coming to office in January 1993, President Clinton added to the corporate espionage machine by creating the National Economic Council, which feeds intelligence to "select" companies to enhance US competitiveness. The capabilities of ECHELON to spy on foreign companies is nothing new, but the Clinton Administration has raised its use to an art.

In 1990, the German magazine *Der Spiegel* revealed that the NSA had intercepted messages about an impending $200 million deal between Indonesia and the Japanese satellite manufacturer NEC Corp. After President Bush intervened in the negotiations on behalf of American manufacturers, the contract was split between NEC and AT&T.

In 1994, the CIA and NSA intercepted phone calls between Brazilian officials and the French firm Thomson-CSF about a radar system that the Brazilians wanted to purchase. The US firm Raytheon was a competitor as well, and was forwarded reports prepared from intercepts.[55]

In September 1993, President Clinton asked the CIA to spy on Japanese auto manufacturers that were designing zero-emission cars and to forward that information to the Big Three US car manufacturers: Ford, General Motors and Chrysler.[56] In 1995, the *New York Times* reported that the NSA and the CIA's Tokyo station were involved in providing detailed information to US Trade Representative Mickey Kantor's team of negotiators in Geneva, facing Japanese car companies in a trade dispute.[57] Recently, the Japanese newspaper *Mainichi* accused the NSA of continuing to monitor the communications of Japanese companies on behalf of American companies.[58]

*Insight* magazine reported in a series of articles in 1997 that President Clinton ordered the NSA and FBI to mount a massive surveillance operation at the 1993 Asia-Pacific Economic Co-operation (APEC) conference, held in Seattle. One intelligence source for the story related that over 300 hotel rooms had been bugged for the event—a move which was designed to obtain information regarding oil and hydro-electric deals pending in Vietnam, that was passed on to high-level Democratic Party contributors competing for the contracts.[59]

But foreign companies were not the only losers. When Vietnam expressed interest in purchasing two used 737 freighter aircraft from an American businessman, the deal was scuttled after Commerce Secretary Ron Brown arranged favourable financing for two new 737s from Boeing.[60]

But the US is not the only partner of the UKUSA relationship which engages in such activity. British Prime Minister Margaret Thatcher ordered the GCHQ to monitor the activities of international media mogul Robert Maxwell on behalf of the Bank of England.[61]

Former CSE linguist and analyst Jane Shorten claimed that she had seen intercepts from Mexican trade representatives during the 1992–1993 NAFTA trade negotiations, as well as 1991 South Korean Foreign Ministry intercepts dealing with the construction of three Canadian CANDU nuclear reactors for the Koreans in a US$6 billion deal.[62] Shorten's revelation prompted Canadian Deputy Prime Minister Sheila Copps to launch a probe into the allegations after the Mexicans lodged a protest.

But every spy agency eventually gets beat at its own game. Mike Frost relates in *Spyworld* how an accidental cellphone intercept in 1981, of the American Ambassador to Canada discussing a pending grain deal that the US was about to sign with China, provided Canada with the American negotiating strategy for the deal. The information was used to outbid the US, resulting in a three-year, $2.5-billion contract for the Canadian Wheat Board. CSE out-spooked the NSA again a year later when Canada snagged a $50-million wheat sale to Mexico.[63]

Another disturbing trend regarding the present commercial use of ECHELON is the incestuous relationship that exists between the intelligence agencies and the US corporations that develop the technology that fuels their spy systems. Many of the companies that receive the most important commercial intercepts—Lockheed, Boeing, Loral, TRW and Raytheon—are actively involved in the manufacturing and operation of many of the spy systems that comprise ECHELON.

The collusion between intelligence agencies and their contractors is frightening in the chilling effect it has on creating any foreign or even domestic competition. But just as important is that it is a gross misuse of taxpayer-financed resources.

## THE WARNING

While the UKUSA relationship is a product of Cold War political and military tensions, ECHELON is purely a product of the 20th century—the century of "statism". The modern drive toward the assumption of state power has turned legitimate national security agencies and apparati into pawns in a manipulative game, where the stakes are no less than the survival of the Constitution. The systems developed prior to ECHELON were designed to confront the expansionist goals of the Soviet Empire—something the West was forced out of necessity to do.

But as Glyn Ford, European Parliament representative for Manchester, England, and the driving force behind the European investigation of ECHELON, has pointed out: "The difficulty is that the technology has now become so elaborate that what was originally a small client list has become the whole world."[64]

What began as a noble alliance to contain and defeat the forces of communism has turned into a *carte blanche* to disregard the rights and liberties of the American people and the population of the free world. As has been demonstrated time and again, the NSA has been persistent in subverting not just the *intent* of the law in regard to the prohibition of domestic spying, but the *letter* as well. The laws that were created to constrain the intelligence agencies from infringing on our liberties are frequently flaunted, re-interpreted and revised according to the bidding and wishes of political spymasters in Washington, DC. Old habits die hard, it seems.

**"The difficulty is that the technology has now become so elaborate that what was originally a small client list has become the whole world."**

Glyn Ford,
European Parliament representative
for Manchester, England

As stated above, there is a need for such sophisticated surveillance technology. Unfortunately, the world is filled with criminals, drug lords, terrorists and dictators who threaten the peace and security of many nations. The thought that ECHELON can be used to eliminate or control these international thugs is heartening. But defenders of ECHELON argue that the rare intelligence victories over these forces of darkness and death give wholesale justification to indiscriminate surveillance of the entire world and every member of it. But more complicated issues than that remain.

The shameless and illegal targeting of political opponents, business competitors, dissidents and even Christian ministries stands as a testament that if we are to remain free, we must bind these intelligence systems and those that operate them with the heavy chains of transparency and accountability to our elected officials. But the fact that the ECHELON apparatus can be quickly turned around on those same officials in order to maintain some advantage for the intelligence agencies indicates that these agencies are not presently under the control of our elected representatives.

That Congress is not aware of or able to curtail these abuses of power is a frightening harbinger of what may come here in the United States. The European Parliament has begun the debate over what ECHELON is, how it is being used and how free countries should use such a system. The US Congress should join that same debate with the understanding that the consequences of ignoring or failing to address these issues could foster the demise of our republican form of government. Such is the threat, as Senator Frank Church warned the American people over twenty years ago:

*At the same time, that capability at any time could be turned around on the American people and no American would have any privacy left, such [is] the capability to monitor everything: telephone conversations, telegrams, it doesn't matter. There would be no place to hide. If this government ever became a tyranny, if a dictator ever took charge in this country, the technological capacity that the intelligence community has given the government could enable it to impose total tyranny, and there would be no way to fight back, because the most careful effort to combine together in resistance to the government, no matter how privately it was done, is within the reach of the government to know. Such is the capability of this technology…*

*I don't want to see this country ever go across the bridge. I know the capacity that is there to make tyranny total in America, and we must see to it that this agency and all agencies that possess this technology operate within the law and under proper supervision, so that we never cross over that abyss. That is the abyss from which there is no return.*[65]

## RECENT DEVELOPMENTS

Since this author's ECHELON report was first sent to the US Congress in November 1998, increased attention has been directed at the spy system by international media outlets and governmental representatives. As news of the system's sweeping technological capability comes to light, questions continue to be raised concerning the possible illicit uses of the system to circumvent domestic civil liberties protections.

The May 1999 publication of British investigator Duncan Campbell's detailed report, "Interception Capabilities 2000", for the European Parliament's Science and Technology Options Assessment Panel (STOA) continued to expose the scope of ECHELON's supporting facilities and the reach of its surveillance technology. Among the report's key findings:[66]

• While "word spotting" search systems have been previously thought to be widespread throughout the system, evidence indicates that this nascent technology is currently ineffective. However, ECHELON utilises speaker recognition system "voiceprints" to recognise the speech patterns of targeted individuals making international telephone calls.

• US law enforcement agencies are working with their European counterparts under the auspices of a previously secret organisation, ILETS (International Law Enforcement Telecommunications Seminar), to incorporate backdoor wiretapping capabilities into all existing forms of communications systems. In addition, the US Government is continuing to pursue diplomatic initiatives to convince other governments to adopt "key escrow" legislation requiring computer users to provide law enforcement agencies with encryption keys.

• The NSA continues to work with US software manufacturers to weaken the cryptographic capability of popular software programs, such as Lotus Notes and Internet browsers, to assist the

**Continued on page 83**

Continued from page 23

intelligence agency in gaining access to a user's personal information.

• Intelligence sources reveal the increasing use of signals intelligence facilities to provide commercial advantages to domestic companies involved in international trade deals.

The report provides original, new documentation about the ECHELON system and its role in the interception of communications satellites. This includes details concerning how intelligence agencies are able to intercept Internet traffic and digital communications, including screen shots of traffic analysis from NSA computer systems.

### Official UKUSA Confirmation

Privacy researchers were surprised in May when an Australian intelligence official confirmed the existence of the UKUSA intelligence-sharing treaty, in response to a formal information request by Channel 9 *Sunday* reporter Ross Coulthart. Martin Brady, director of the Defence Signals Directorate (DSD), admitted in a letter dated 16 March that his agency "does cooperate with counterpart signals intelligence organisations overseas under the UKUSA relationship".[67]

### Parliamentary and Congressional Inquiries

The growing concern about the use of ECHELON has finally extended to capitals and elected representatives around the world. Pressure from the international business community has been brought to bear on government officials in response to mounting evidence that industrial espionage by the US is costing European firms billions of dollars each year.

Germany also followed the French example in June, when the cabinet issued a policy statement encouraging its companies and citizens to utilise encryption programs without restrictions. German business leaders were alerted to the extent of US commercial spying after an anonymous NSA employee admitted on German television in August 1998 that he had participated in stealing industrial secrets from the wind generator manufacturer, Enercon, which were passed on to its main US competitor, Kenetech.[68]

Perhaps the most important governmental development is the growing interest of members of the US Congress regarding ECHELON and its surveillance capabilities. Since the NSA is the prime mover in the UKUSA intelligence partnership, any hope of reining-in the activities of the US intelligence agencies will require the involvement of congressional oversight committees.[69] ∞

### Endnotes

32. *Brown v. Glines*, 444 US 348 (1980).
33. Bamford, James, *The Puzzle Palace: Inside the National Security Agency, America's Most Secret Intelligence Organization*, Penguin Books, New York, 1983, pp. 314, 459.
34. External Collection Program, US Senate, Select Committee on Intelligence, "Supplementary Detailed Staff Reports on Intelligence and the Rights of Americans", Final Report, Book III, April 23, 1976, p. 765.
35. *United States v. United States District Court*, 407 US 297 (1972).
36. Bamford, ibid., pp. 370-373.
37. Ibid., p. 381.
38. Halperin, Morton, Berman, Jerry et al., *The Lawless State*, Penguin, New York, 1976, p. 146.
39. Hersh, Seymour, "Huge CIA Operation Reported in US Against Antiwar Forces", *New York Times*, December 22, 1974, p. 1.

Continued on page 85

**Continued from page 83**

40. Halperin and Berman, p. 153; US Commission on CIA Activities within the United States, *Report to the President*, US Government Printing Office, Washington, DC, 1975, p. 144n3.
41. 50 USC Sec. 1801, et seq.
42. For more information on the FISC, refer to this author's essay, "Inside America's Secret Court: The Foreign Intelligence Surveillance Court", *The Privacy Papers*, No. 2, Free Congress Foundation, Washington, DC, 1998, posted at author's website, at <http://fly.hiwaay.net/~pspoole/fiscshort.html>.
43. Frost, Mike and Gratton, Michel, *Spyworld: How CSE Spies on Canadians and the World*, Seal/McClelland-Bantam, Toronto, 1995, pp. 234-238.
44. Ibid., p. 238.
45. Ibid., pp. 93-97.
46. Shane, Scott and Bowman, Tom, "Catching Americans in NSA's Net", Baltimore *Sun*, December 12, 1995.
47. Epstein, Keith C. and Long, John S., "Security Agency Accused of Monitoring US Calls", Cleveland *Plain Dealer*, July 1, 1988, pp. 1A, 10A.
48. Carey, Pete, "NSA Accused of Forbidden Phone Taps", San Jose *Mercury News*, July 2, 1988, p. 1A.
49. Campbell, Duncan, "Somebody's Listening", *The New Statesman*, August 12, 1988, p. 11.
50. Shane and Bowman, ibid.
51. Ibid.
52. Merritt, John, "UK: GCHQ Spies on Charities and Companies: Fearful Whistleblowers Tell of Massive Routine Abuse", *Observer*, London, June 18, 1992.
53. O'Shaughnessy, Hugh, "Thatcher Ordered Lonrho Phone-Tap Over Harrods Affairs", *Observer*, London, June 28, 1992; cited in Hager, Nicky, *Secret Power: New Zealand's Role in the International Spy Network*, Craig Potton Publishing, Nelson, New Zealand, 1996, p. 54.
54. "The Hill", *Dispatches*, BBC Channel 4, October 6, 1993.
55. Bowman, Tom and Shane, Scott, "Battling High-Tech Warriors," Baltimore *Sun*, December 15, 1995.
56. Dreyfuss, Robert, "Company Spies", *Mother Jones*, May/June 1994.
57. Cited in Livesey, Bruce, "Trolling for Secrets: Economic Espionage is the New Niche for Government Spies", *Financial Post*, Canada, February 28, 1998.
58. "US Spy Agency Helped US Companies Win Business Overseas", *Nikkei English News*, September 21, 1998.
59. Maier, Timothy W., "Did Clinton Bug Conclave for Cash?", *Insight*, September 15, 1997. The three-article series is online at <http://www.insightmag.com/investiga/apecindex.html>.
60. Maier, Timothy W., "Snoops, Sex and Videotape", *Insight*, September 29, 1997.
61. Fletcher, Matthew, "Cook Faces Quiz on Big Brother Spy Net", *Financial Mail*, UK, March 1, 1998.
62. Livesey, op. cit.
63. Frost and Gratton, ibid., pp. 224-227.
64. Redmond, Lucille, "Suddenly There Came a Tapping…", *The Sunday Business Post*, Ireland, March 9, 1998.
65. National Broadcasting Company, "Meet the Press", August 17, 1975; transcript published by Merkle Press, Washington, DC, 1975, p. 6; quoted in Bamford, p. 477.
66. The full report can be found online at: <www.iptvreports.mcmail.com/interception_capabilities.htm>.
67. See <http://sunday.ninemsn.com.au/sun_cover2.asp?id=818>.
68. Paterson, Tony, "US spy satellites 'raiding German firms' secrets'", *The Sunday Telegraph*, London, April 11, 1999.
69. Verton, Daniel, "Congress, NSA butt heads over ECHELON", *Federal Computer Week*, June 3, 1999, <www.fcw.com/pubs/fcw/1999/0531/web-nsa-6-3-99.html>.

**About the Author:**

Patrick S. Poole is a lecturer in government and economics at Bannockburn College in Franklin, Tennessee, USA, having previously served as Deputy Director of the Center for Technology Policy in Washington, DC. He contributes frequently to several publications on the topics of privacy and civil liberties.